

RECEIVED
CENTRAL FAX CENTER

MAR 21 2006

DILLON & YUDELL LLP
ATTORNEYS AT LAW

USPTO FACSIMILE TRANSMITTAL SHEET

TO:	FROM:
Examiner Christopher Brown	James E. Boice, Reg. No. 44,545
ORGANIZATION:	DATE:
US Patent and Trademark Office	March 21, 2006
ART UNIT:	TOTAL NO. OF PAGES INCLUDING COVER:
2134	14
FAX NUMBER:	APPLICATION SERIAL NO:
571.273.8300	10/062,348
ENCLOSED:	ATTORNEY DOCKET NO:
Appeal Brief	AUS920010978US1

☒ URGENT ☐ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

This fax from the law firm of Dillon & Yudell LLP contains information that is confidential or privileged, or both. This information is intended only for the use of the individual or entity named on this fax cover letter. Any disclosure, copying, distribution or use of this information by any person other than the intended recipient is prohibited. If you have received this fax in error, please notify us by telephone immediately at 512.343.6116 so that we can arrange for the retrieval of the transmitted documents at no cost to you.

8911 N. CAPITAL OF TEXAS HWY., SUITE 2110, AUSTIN, TEXAS 78759
512.343.6116 (V) • 512.343.6446 (F) • DILLONYUDELL.COM

RECEIVED
CENTRAL FAX CENTER

MAR 21 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

IN RE APPLICATION OF:

DAVID YU CHANG, ET AL.

SERIAL NO.: 10/062,348

FILED: 31 JANUARY 2002

FOR: MULTIPLE SECURE
SOCKET LAYER KEYFILES
FOR CLIENT LOGIN
SUPPORT

ATTY. DOCKET NO.:

AUS920010978US1

§
§
§
§
§
§
§
§
§
§

EXAMINER: CHRISTOPHER J. BROWN

ART UNIT: 2134

APPEAL BRIEF UNDER 37 C.F.R. 41.37Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Brief is submitted in support of the Appeal of the Examiner's final rejection of Claims 1-12 in the above-identified application. A Notice of Appeal was filed in this case on February 24, 2006 and received in the United States Patent and Trademark Office on February 24, 2006. Please charge the fee of \$500.00 due under 37 C.F.R. §1.17(c) for filing the brief, as well as any additional required fees, to **IBM CORPORATION DEPOSIT ACCOUNT No. 09-0447**.

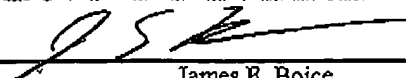
CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(A)]

I hereby certify that this correspondence is being:

☐ deposited with the U.S. Postal Service on the date shown below with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.☒ transmitted by facsimile on the date shown below to the U.S. Patent and Trademark Office at (571) 273-8300.

3-21-6

Date



James E. Boice

AUS920010978US1 - Appeal Brief

- 1 -

Serial No. 10/062,348

REAL PARTY IN INTEREST

The real party in interest in the present Application is International Business Machines Corporation, the Assignee of the present application as evidenced by the Assignment set forth at reel 012576, frame 0214.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-12 stand finally rejected by the Examiner as noted in the Final Office Action dated December 9, 2005. The rejection of Claims 1, 5 and 9 under 35 U.S.C. § 112, first and second paragraphs; and the rejection of Claims 1-12 under 35 U.S.C. § 103(a) are appealed.

STATUS OF AMENDMENTS

No amendments to the claims have been made subsequent to the December 9, 2005 Final Office Action from which this Appeal is filed.

SUMMARY OF THE CLAIMED SUBJECT MATTER

As recited by Appellants' independent **Claim 1**, Appellants' invention provides a method for establishing a secure connection to a server for a specific user of a client computer on a network utilizing a Secure Sockets Layer (SSL) system. The method comprises the following steps:

(1) storing a plurality of keyfiles for different users in a data storage that is accessible only to a client computer, each of said keyfiles comprising a unique private cryptology key, a corresponding public cryptology key, and a name of a Certificate Authority (CA) that issued the unique private cryptology key and the corresponding public cryptology key for a specific user;

(2) storing a plurality of passwords in said data storage, each of said passwords being associated with a respective keyfile, each of said passwords being capable of opening only one of said keyfiles;

(3) in response to receiving one of said passwords input from the specific user, opening said one of said keyfiles associated with said one of said passwords and said specific user; and

(4) transmitting from said client computer to a server a digital certificate from said open keyfile to enable said server to authenticate an identity of said specific user from a plurality of users who are authorized to use said client computer, wherein a secure connection is established with the server for the specific user.

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

- A. The Examiner's rejection of Claims 1, 5 and 9 under 35 U.S.C. § 112, first paragraph, is to be reviewed on Appeal.
- B. The Examiner's rejection of Claims 1, 5 and 9 under 35 U.S.C. § 112, second paragraph, is to be reviewed on Appeal.
- C. The Examiner's rejection of Claims 1, 2, 4-6, 8-10 and 12 as being unpatentable under 35 USC 103(a) over *Wrench Jr.* (U.S. Patent Application Publication No. 2002/0104025 – “*Wrench*”) in view of *Sasaki, et al.* (U.S. Patent No. 6,378,071 – “*Sasaki*”) and *Schneier's* publication “Applied Cryptography” (*Schneier*); and Claims 3, 7 and 11 under 35 USC 103(a) over *Wrench* in view of *Sasaki* and *Schneier* and *Norris, et al.* (U.S. Patent Application Publication No. 2002/0095568 – “*Norris*”), is to be reviewed on Appeal.

ARGUMENTS

A. The Examiner's rejection of Claims 1, 5 and 9 under 35 U.S.C. § 112, first paragraph.

The Examiner's rejection of Claims 1, 5 and 9 is improper since the phrases "data storage that is accessible only to a client computer" and "opening only one of said keyfiles" are supported by the specification.

The Examiner has rejected Claims 1, 5 and 9, stating that the limitation "storing a plurality of keyfiles for different users in a data storage that is accessible only to a client computer" is not supported by the specification. However, this feature is supported, *inter alia*, on page 12, lines 21-26, of the present specification, which discusses protecting access to keyfiles. Specifically, the specification states that a user must enter a password to access the data storage via a GUI on "display 32 using GUI application 40, shown in Figures 3 and 4, respectively, for the user's password 22 that will unlock that user's keyfile 24 containing the user's digital certificate and private key found in authentication data 42 as described in Figure 4." Thus, since only a local input to the client computer will be afford access to the keyfiles, then the data storage is accessible only to the client computer.

The Examiner has also rejected Claims 1, 5 and 9, stating that the limitation "each of said passwords being capable of opening only one of said keyfiles" is not supported by the specification. However, this feature is supported, *inter alia*, on page 12 line 8, in which "Each of the multiple users has a unique keyfile 24." As stated on page 10, lines 10-12, the "user identified by user identifier 15a ("User ID 1") enters password 22a ("Password1") to open keyfile 24a ("Keyfile 1"). Thus each of the passwords is "capable of opening only one of said keyfiles," such that "in response to receiving one of said passwords input from the specific user, opening said one of said keyfiles associated with said one of said passwords and said specific user."

Thus, this rejection is not well founded and should be reversed.

- B. The Examiner's rejection of Claims 1, 5 and 9 under 35 U.S.C. § 112, second paragraph.

The Examiner's rejection of Claims 1, 5 and 9 is improper since the phrase "the specific user" has support in the preambles of the claims.

The Examiner has rejected Claims 1, 5 and 9 for lack of antecedent basis of the term "the specific user." However, the term "a specific user," to which the term "the specific user" refers, is found in the preamble of the claim, and thus has sufficient antecedent basis. (MPEP 706.03(d))

Thus, this rejection is not well founded and should be reversed.

- C. The Examiner's rejection of Claims 1, 2, 4-6, 8-10 and 12 as being unpatentable under 35 USC 103(a) over *Wrench Jr.* (U.S. Patent Application Publication No. 2002/0104025 – "*Wrench*") in view of *Sasaki, et al.* (U.S. Patent No. 6,378,071 – "*Sasaki*") and *Schneier's* publication "Applied Cryptography" (*Schneier*); and Claims 3, 7 and 11 under 35 USC 103(a) over *Wrench* in view of *Sasaki* and *Schneier* and *Norris, et al.* (U.S. Patent Application Publication No. 2002/0095568 – "*Norris*").

The Examiner's rejection of Claims 1-12 is improper since the cited prior art does not teach or suggest all of the limitations of the claims.

With reference to exemplary Claim 1, the cited art does not teach or suggest the limitation of "storing a plurality of keyfiles for different users in a data storage that is accessible only to a client computer." *Sasaki* teaches in Figure 3, and col. 5, lines 40-45, that the CPU in the client computer is to "determine whether the input user ID and password accords with a registered user ID and password." However, there is no teaching or suggestion of the limitation that the data storage is accessible only to the client computer. Rather, in *Sasaki* the data storage may be accessible through any client computer, as long as the user knows the correct user ID and password.

Furthermore, the cited art does not teach the limitations of “storing a plurality of keyfiles for different users” and “in response to receiving one of said passwords input from the specific user, opening said one of said keyfiles associated with said one of said passwords and said specific user” (i.e., each of the keyfiles are password protected for a specific user). This feature is supported, *inter alia*, by Figure 4 and the related text. While *Wrench* teaches that a private key may be password protected (paragraph [0028]), there is no suggestion of storing a different keyfile for each of a plurality of different users. Similarly, while *Sasaki* teaches that a password and ID checker (user authentication unit 2) may check to see if a password and ID are correct for opening a file, there is no suggestion of multiple “users” having different “keyfiles.” Thus, this feature is not taught or suggested by the cited art.

As the cited art does not teach or suggest all of the limitations of the presently claimed invention, this rejection is not well founded and should be reversed.

CONCLUSION

Appellants have pointed out with specificity the manifest error in the Examiner's rejections, and the claim language which renders the invention patentable over the various combinations of references. Appellants, therefore, respectfully request that this case be remanded to the Examiner with instructions to issue a Notice of Allowance for all pending claims.

Respectfully submitted,



James E. Boice
Reg. No. 44,545
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANTS

CLAIMS APPENDIX

1. A method for establishing a secure connection to a server for a specific user of a client computer on a network utilizing a Secure Sockets Layer (SSL) system, said method comprising:

storing a plurality of keyfiles for different users in a data storage that is accessible only to a client computer, each of said keyfiles comprising a unique private cryptology key, a corresponding public cryptology key, and a name of a Certificate Authority (CA) that issued the unique private cryptology key and the corresponding public cryptology key for a specific user;

storing a plurality of passwords in said data storage, each of said passwords being associated with a respective keyfile, each of said passwords being capable of opening only one of said keyfiles;

in response to receiving one of said passwords input from the specific user, opening said one of said keyfiles associated with said one of said passwords and said specific user; and

transmitting from said client computer to a server a digital certificate from said open keyfile to enable said server to authenticate an identity of said specific user from a plurality of users who are authorized to use said client computer, wherein a secure connection is established with the server for the specific user.

2. The method of claim 1, further comprising:

storing an authentication data for said specific user in said data storage, said authentication data comprising a unique identifier that corresponds to a password for said specific user; and

identifying said specific user for opening a keyfile according to said unique identifier.

3. The method of claim 1, further comprising:

authenticating an identity of said specific user through a process of hashing, said process including the steps of:

hashing a message into a hashed message using a hash function;

encrypting said hashed message into an encrypted hashed message using said private cryptology key; and

transmitting said hash function, said message and said encrypted hashed message to said server.

4. The method of claim 1, further comprising prompting said specific user for a password through a Graphical User Interface (GUI) in a display associated with said client computer.

5. A client computer for establishing a secure connection to a server for a specific user of the client computer on a network utilizing a Secure Sockets Layer (SSL) system, said client computer comprising:

means for storing a plurality of keyfiles for different users in a data storage that is accessible only to a client computer, each of said keyfiles comprising a unique private cryptology key, a corresponding public cryptology key, and a name of a Certificate Authority (CA) that issued the unique private cryptology key and the corresponding public cryptology key for a specific user;

means for storing a plurality of passwords in said data storage, each of said passwords being associated with a respective keyfile, each of said passwords being capable of opening only one of said keyfiles;

means for, in response to receiving one of said passwords input from the specific user, opening said one of said keyfiles associated with said one of said passwords and said specific user; and

means for transmitting from said client computer to a server a digital certificate from said open keyfile to enable said server to authenticate an identity of said specific user from a plurality of users who are authorized to use said client computer, wherein a secure connection is established with the server for the specific user.

6. The client computer of claim 5, further comprising:

means for storing an authentication data for said specific user in said data storage, said authentication data comprising a unique identifier that corresponds to a password for said specific user; and

means for identifying said specific user for opening a keyfile according to said unique identifier.

7. The client computer of claim 5, further comprising:

means for authenticating the identity of said specific user through a process of hashing, said means for authenticating the identity of said specific user through said process of hashing including:

means for hashing a message into a hashed message using a hash function;

means for encrypting said hashed message into an encrypted hashed message using said private cryptology key; and

means for transmitting said hash function, said message and said encrypted hashed message to said server.

8. The client computer of claim 5, further comprising means for prompting said specific user for a password through a Graphical User Interface (GUI) in a display associated with said client computer.

9. A computer program product residing on a computer usable medium for establishing a secure connection to a server for a specific user of a client computer on a network utilizing a Secure Sockets Layer (SSL) system, said computer program product comprising:

program code means for storing a plurality of keyfiles for different users in a data storage that is accessible only to a client computer, each of said keyfiles comprising a unique private cryptology key, a corresponding public cryptology key, and a name of a Certificate Authority (CA) that issued the unique private cryptology key and the corresponding public cryptology key for a specific user;

program code means for storing a plurality of passwords in said data storage, each of said passwords being associated with a respective keyfile, each of said passwords being capable of opening only one of said keyfiles;

program code means for, in response to receiving one of said passwords input from the specific user, opening said one of said keyfiles associated with said one of said passwords and said specific user; and

program code means for transmitting from said client computer to a server a digital certificate from said open keyfile to enable said server to authenticate an identity of said specific user from a plurality of users who are authorized to use said client computer, wherein a secure connection is established with the server for the specific user.

10. The computer program product of claim 9, further comprising:

program code means for storing an authentication data for said specific user in said data storage, said authentication data comprising a unique identifier that corresponds to a password for said specific user; and

program code means for identifying said specific user for opening a keyfile according to said unique identifier.

11. The computer program product of claim 9, further comprising:

program code means for authenticating the identity of the specific user through a process of hashing, said program code means including:

program code means for hashing a message into a hashed message using a hash function;

program code means for encrypting said hashed message into an encrypted hashed message using said private cryptology key; and

program code means for transmitting said hash function, said message and said encrypted hashed message to said server.

12. The computer program product of claim 9, further comprising:

program code means for displaying a Graphical User Interface (GUI) in a display associated with said client computer; and

program code means for prompting said specific user for a password through said GUI.

EVIDENCE APPENDIX

Other than the Office Action(s) and reply(ies) already of record, no additional evidence has been entered by Appellants or the Examiner in the above-identified application which is relevant to this appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings as described by 37 C.F.R. §41.37(c)(1)(x) known to Appellants, Appellants' legal representative, or assignee.